

FREQUENTLY ASKED QUESTIONS

OVERVIEW

1. What exactly is the P.i.E Programme?

It stands for Privacy in Education, an exclusive compliance support initiative by Securys Jamaica in partnership with the Jamaica Independent Schools Association (JISA). The programme offers a privacy posture and exposure review, Data Protection Officer as a Service (DPOaaS), tailored remediation plans and streamlined digital onboarding. This is all geared at helping independent schools meet all their obligations under Jamaica's Data Protection Act (2020).

2. Why is the Jamaica Data Protection Act (JDPA) applicable to my school?

Due to the nature of the data that is processed by schools, the JDPA recognizes schools as part of a priority group. This means that schools have a heightened responsibility to be compliant with the JDPA by ensuring they implement a robust privacy framework to protect the information they process for staff, parents and their students.

3. Is this programme mandatory, or just recommended?

The programme itself is optional, but compliance with the Jamaica Data Protection Act, 2020 is mandatory. P.i.E. is simply a practical and affordable way for schools to meet their legal obligations without having to build everything from scratch.

4. Why should schools act now?

Jamaica's Data Protection Act (DPA) took effect in 2023, and schools must be able to demonstrate compliance. Primarily, this includes registering with the Office of the Information Commissioner, appointing a qualified Data Protection Officer, adopting safeguards including training and documented risk assessments to protect personal data, annual filing of Data Privacy Impact Assessments as well as re-registering annually, among other obligations.

5. How do I explain this to my board or school owners?

It's best to think of it as both insurance and good governance. Just as we are expected to insure our buildings and buses, we must now protect student and staff information. This programme makes compliance affordable and sector-specific, so the school avoids fines, reputational damage and legal risk.

6. Where can we learn more about the DPA and compliance for schools?

You can access the webinars and insights from Securys and JISA, at www.securys.com.jm/pie

WHAT MAKES IT DIFFERENT?

7. What makes P.i.E different from other options?

This is a sector-exclusive offer for JISA-affiliated schools – not available on the open market. It's designed to spread cost across participants, making it more affordable and deeper in service than anything else on offer.

8. How is this different from hiring a lawyer or IT consultant?

Lawyers and IT specialists handle only pieces of the challenge. P.i.E. combines legal, technical and operational expertise in one package. Instead of juggling multiple vendors and staff, schools get a single, affordable solution that covers all requirements.

PROGRAMME DETAILS

9. What is included in the P.i.E support?

Schools will benefit from:

- Comprehensive privacy policies and notices tailored to educational needs and suited to both regulatory compliance and comprehension by staff, parents and students.
- Completion of required risk assessments and associated regulatory documentation.
- Annual registration of your school with the O.I.C.
- Registration of Securys Jamaica as your statutory Data Protection Officer.
- Submission of your annual Data Protection Impact Assessment to the O.I.C.
- Management of interactions with the regulator and with data subjects, including responding to data subject access requests and other exercises of data subject rights under the Jamaica Data Protection Act.
- Management, in collaboration with your staff and IT function, of any data breaches, including regulatory and data subject communication.
- Provision of ongoing training for staff in all aspects of data protection as it pertains to education and the protection of children's and young persons' data.

10. What exactly does the DPO do?

The DPO monitors compliance, advises the school on its obligations, trains staff, files required reports and acts as the contact point with the OIC and with data

subjects (staff, students, parents, contractors and other stakeholders).

11. Why can't I just name one of my teachers or admin staff as the DPO?

The law requires the DPO to be independent and qualified. If you appoint staff, they risk conflicts of interest and may not have the expertise. Outsourcing ensures compliance and avoids liability.

12. If we join P.i.E., do we still need to hire a DPO internally?

No. Provision of a registered statutory DPO is included in P.i.E. You do not need to appoint someone else internally.

13. Will the DPO visit my school regularly in person or only work remotely?

Most work is done remotely for efficiency, with opportunities to visit in person as needed for audits, training or sensitive issues.

TIMELINE AND COHORTS

14. When does the programme begin, and what are the cohorts?

- **Cohort 1:** For agreements signed and returned before August 29, 2025, with engagement starting at the beginning of October 2025,
 - **Cohort 2:** Signed after August 29, 2025, onboarding begins January 2026.
- Further cohorts will follow each semester.**

15. What if we're past the deadline for Cohort 1?

If you miss the August deadline, the next intake will be January 2026.

COST & BUDGETING

16. Is there any cost to register initially?

No payment is required when signing up or completing the digital onboarding questionnaire.

17. What about long-term budgeting and pricing?

The P.i.E. programme offers fixed pricing over five years, aligned with academic cycles – this gives schools predictable, budget-friendly planning.

18. Do smaller schools pay less than larger ones?

Yes. Fees are scaled to the size of your school community, so smaller schools pay less than larger ones. This makes compliance fair and affordable across the sector.

19. Do I start paying immediately?

No, you do not. After sending in your signed proposal, as part of your onboarding process, we will discuss your preferred billing method. You get to choose how you pay.

20. What are the payment plan options available?

We offer monthly, per semester and annual payment options. If you would prefer an alternate payment option, we would be happy to have a further conversation with each school.

21. Will there be any other costs?

The only additional cost will be your annual registration fee, payable directly to the OIC when we submit your registration. This fee is presently either JM\$15,000 or JM\$25,000 for the initial registration, depending on the constitution of your school, and either JM\$10,000 or JM\$15,000 for each subsequent year.

COMPLIANCE AND LEGAL IMPLICATIONS

22. Will this be recognized by the regulator (OIC) as acceptable compliance?

Yes. This OIC does not endorse specific providers, but everything in P.i.E. is aligned with the law. The services – appointing a qualified DPO, filing mandatory reports and implementing safeguards – are exactly what the regulator requires.

23. Will this programme file our registration with the regulator for us?

Yes. P.i.E. includes support for preparing and filing your registration with the OIC to ensure it is done properly and on time. You will need to pay the registration fee to the OIC directly.

24. What is this Data Privacy Impact Assessment we keep hearing about and why should this be filed annually?

The DPIA is similar to a safety check for how your school collects and uses data. The law requires that you review risks every year and file a Data Privacy Impact Assessment (DPIA) starting March 2026. This ensures you stay compliant as your school grows and changes.

25. Could my school or I personally be fined or sued?

Yes. The school can be fined up to 4% of annual revenue and in some cases principals or board members can be held personally liable.

26. Will this affect our inspection reports from the Ministry of Education?

Yes, indirectly. Data protection is part of overall governance and safeguarding.

Inspectors are likely to ask about compliance, especially around student safety and record-keeping.

IMPACT AND WORKLOAD

27. How much extra work will this mean for me and my staff?

The programme is designed to minimise extra work. Most of the heavy lifting is done by the Securys team. Your staff will only need to complete training and follow the policies put in place.

28. Do we need to buy new software or IT systems?

No. Most schools can comply using their existing systems once safeguards are added. If upgrades are needed, we'll guide you towards simple, affordable options.

ROLES & STAKEHOLDERS

29. Who from my staff should be the main point of contact with Securys?

Usually, your principal, bursar or senior administrator – someone with authority to oversee compliance. They don't need to be a data expert, just a reliable point of contact.

30. What support will staff, parents and students receive?

The programme includes staff training, awareness workshops and sensitization sessions with stakeholders like parents, students and suppliers to nurture a culture of privacy.

31. Will my staff have to attend long workshops?

No. Training is short, practical and tailored for schools. It's designed to fit into busy schedules.

32. Do you train teachers, or only administrators?

Both. Everyone who handles personal data, including teachers, must have some training. Administrators and leadership receive deeper sessions.

SECTOR BENEFITS

33. How does joining early benefit all schools?

Early participation helps:

- Maintain low costs for all schools,
- Reinforce sector-wide cost efficiency,
- Demonstrate leadership in ethical data handling and compliance.

NEXT STEPS

34. How can my school register interest?

Complete the Digital Onboarding Questionnaire, and your personalized proposal will follow.

35. I have received my tailored proposal, what now?

Once you have received your tailored proposal, open the discussion with your school's leadership (principal, vice principal or board). Once you have agreed, please sign and return a copy of the proposal to us at info@securys.com.jm.

36. We want to start but don't have the budget. What should we do?

We understand that budget may be a factor. You may communicate with us directly on how you may be able to finance the initiative, and we can arrive at a suitable agreement.

RISK CONSIDERATIONS

37. Are there penalties if we drop out after a year or two?

No financial penalties, but the school would lose access to the benefits of the program and would need to make alternative arrangements for data protection and appointment of a DPO in order to continue operating within the law.

38. Who is responsible if something goes wrong – the DPO or the school?

The school always remains legally responsible. The DPO guides and supports you, but ultimately accountability rests with the school's leadership.

39. What if we decide to do this on our own – why do we need Securys?

You can, but it's expensive and risky. You'd need a qualified DPO, continuous legal advice, IT support and staff training separately. P.i.E combines all of this at a fraction of the cost, with sector-specific expertise.